CHAPTER

2

SERVER PLANNING

After reading this chapter and completing the exercises, you will be able to:

- Determine the most appropriate server solution for a given business purpose
- Plan for user demands on the server
- Consider interoperability among operating systems
- Optimize server placement
- Diagram server plans
- Plan the server environment
- Plan physical site readiness
- Implement sound physical server security practices

The administrator must choose the most appropriate server solution for his or her business environment while also providing adequately for user demand and usage of the server. Sometimes, the administrator's choices involve other mitigating factors such as providing for interoperability between operating systems.

Server administration does not end after the server purchase. You must also place server equipment in optimal locations for both accessibility and disaster prevention. Planning the placement should be documented with accurate and up-to-date diagrams. Server locations must be environmentally fit so that heat, dust, and humidity do not adversely affect server uptime. Finally, the administrator must arrange for the best security available to protect both the hardware investment and the intellectual property that the server data represents.

Determining the Business Purpose

As discussed in Chapter 1, the network administrator must have a business sense of how a server plan directly benefits the organization financially, or indirectly in terms of improving efficiency or productivity. It is obviously the responsibility of the network administrator to obtain necessary network equipment and servers. However, going a step beyond this basic responsibility by contributing to the bottom line of the business will also contribute to your value in the marketplace. Increasingly, organizations see somebody who not only "knows a lot about computers," but also knows how to get the most value for every dollar spent in servicing the network.

Although each organization differs in what benefits its business, the following questions provide a common starting point as you consider if and how a server or servers can improve your organization's business and support its goals.

Do We Really Need This Server Right Now?

As an administrator responsible for thousands (and sometimes millions) of dollars worth of equipment, your IT budget can be substantial. However, you must take server purchases seriously and proceed cautiously, just as if you had a minimal budget. Although this book does not intend to force a financial philosophy, carefully weighing the need for a server against its costs can sometimes help your standing as an administrator. For example, most publicly-traded companies watch the timing of quarterly expenses very carefully. If the company is experiencing less than stellar performance in the quarter, it might not be the best time to propose a large equipment purchase, especially if the purchase is not urgent (i.e., not particularly time-sensitive). You might wait until the beginning of a more promising quarter and attempt to push through equipment approval before anyone has a chance to get nervous!

Conversely, there is little reason to pause before purchasing a vital server. For example, if an email server experiences a catastrophic failure, you would want to replace it (or the failed component) immediately and without apology, because email is a highly utilized function of most organizations and used nearly every second of the workday. In this case, the email server purchase is urgent, and failure to purchase it would negatively impact your standing as an administrator.

In between the urgent and nonurgent equipment purchase comes the "we really could use that pretty soon" purchase. This might be something that does not immediately affect daily productivity or profitability, but for which you can provide reasonable justification. These types of purchases might optimize an existing server plan or proactively save money in the long run. For example, let's say you have a growing research division that is vital to your company's success. The research division can get by on the equipment it currently has, but you often hear about slow access to large user files on the department file server. The network has plenty of available bandwidth and acceptable network utilization, so network issues do not seem to be a problem. (**Bandwidth** is the

transmission capacity of the network. For example, most Ethernet networks can transmit at 10 Mbps or 100 Mbps. **Network utilization** is the percentage of bandwidth in use during a given period of time.) However, you have confirmed that the file server is overutilized. Your solution is to purchase an additional file server to provide **load balancing** by distributing the files between the file servers, effectively halving the burden on the original file server. An additional benefit of load balancing is **failover**—if one of the servers fails, the remaining server(s) continue to provide service. Although you might not be able to specify the exact long-term savings, you can probably present an obvious case for improved productivity and redundancy with the additional file server.

You could also do several other things to increase responsiveness when users access files, such as optimizing external storage or adding more hard disks. These types of solutions are discussed in more detail in later chapters.

Is the Expense of the Server Offset in Savings?

Suppose that your research division also has an office in Denver. You find that researchers in Denver often download large files from file servers in your local research division. The WAN link that connects these two offices is a high, ongoing expense because subscription charges accrue according to usage. (A WAN link is the telecommunications connection that links the various networks that comprise your WAN.) The WAN link is **oversubscribed** (bandwidth utilization is so high that it slows network access), so you want to reduce its usage. In this case, consider adding a file server to the Denver research office that periodically **synchronizes** (updates two or more copies of the same file so that they are the same) with your location's research division. By controlling when this synchronization occurs, you can save bandwidth and lower subscription costs. As an added benefit, the Denver researchers obtain faster access to their file resources. In this case, you can easily justify the addition of the Denver file server against the savings of the oversubscribed WAN link.

Is the Timing of a Server Purchase Appropriate?

Even if budgeting and financial resources are not a concern, the administrator must continue to be careful about the timeliness of a purchase. For example, you might delay the purchase of a new server with the fastest and latest processor even though you require more processing power. If you do not urgently need that much speed now or in the near future, consider other possibilities. For example, if the existing server supports SMP, and you have room for an additional processor, add another processor instead of purchasing an entire server. You might also consider purchasing a server with a processor that is a step or two below the latest and greatest—prices often come down after the release of a new processor.

Is Sufficient Expertise Available to Operate and Maintain the Server?

Sometimes an organization needs a server but does not have anyone available to run and maintain the equipment. This is particularly true in the case of a WAN where multiple, geographically distant locations make it impossible for a network administrator to be everywhere at once. This situation is difficult in that you must supply the server needs of the organization, yet the server cannot run and maintain itself. Although you will probably have to go ahead and provide the server, you might have to budget additional funding to hire outside support services for that office or to fund travel expenses for you to physically visit the server.41

While software exists that allows you to remotely operate a server from your location, such software cannot perform every function. For example, software cannot perform physical actions on the server, such as replacing a power supply.

Anticipating User Demand

It's essential to remember that *the network or systems administrator provides a service to users*. Remembering this responsibility affects the administrator's perspective and job performance. Some administrators find humor in belittling the end user. However, you will be a better administrator if you take the user (a little more) seriously. For example, in asking for a faster Internet connection, users might not understand that they are really asking for another high-speed Internet line and associated equipment costing thousands of dollars per month. The request might or might not be valid. The administrator often helps others (such as members of management) to determine which requests are valid.

The network administrator's job is to ensure that users can perform their jobs in an efficient, timely manner. To do this, he or she may need to wear many "hats," from educator to technician to business manager. The needs in each networking environment vary. However, the following questions might help you as a starting point in servicing user needs.

How Many Users Will Connect to the Server?

This is perhaps the most relevant issue in providing a server for user access. If you anticipate only a few users, you could use virtually any kind of server for general purposes, such as a desktop PC server. However, if you expect frequent access to the server from a large number of users, a more capable midrange computer might be more appropriate with the fastest network card that your network design supports. For example, a large corporation with a company intranet might have several midrange computers serving as intranet web servers. (Multiple web servers providing the same web content are collectively referred to as a **web farm**.)

A **network interface card (NIC)** is the computer's adapter card that connects to the network and through which network communication takes place. Consider installing two or more NICs in highly utilized servers. This multiplies the effective network I/O to and from the server by the number of NICs you install. For example, three NICs provide three times the network I/O capacity of a single NIC, provided the network bandwidth is not oversubscribed.

What Is the Nature of the User Access?

You might have only a few dozen users who, because of their access needs, require a more powerful server than hundreds of users with a different type of access requirement. For example, a few dozen users frequently performing complex and demanding queries on a very large database might require a server with significant storage and processing power. However, hundreds of users requiring a simple logon server probably do not need a significantly powerful server. Later in this book you will learn more about various services and applications, some of which require more powerful hardware than others.

Should Users Be Able to Access the Server Directly?

Some servers are not designed for direct user access. For example, in a Transmission Control Protocol/Internet Protocol (TCP/IP) network, a Dynamic Host Configuration Protocol (DHCP) server assigns unique identification to each computer on the network. This function requires minimal processing, memory, and hard disk storage, and a fairly bland server in terms of power can probably service hundreds of computers. This type of server requires no direct access on the user's part. As a rule, assume that users do not require direct server access and take measures to prevent such access unless you know users or groups of users who require a specific level of access. Also, user access to the server should only be from workstations across the network; users should never log on locally to a server.

Planning for Interoperability

Many network environments use multiple operating systems across their servers and clients (see Figure 2-1). Reasons for this mixture vary. Perhaps two companies with differing operating systems merge, or a particular application only works with one NOS but you want to use the features of another NOS. The administrator must ensure that different operating system platforms can operate with one another and that the user experience is not disrupted. Ideally, the user has no idea that two or more operating systems are in use.

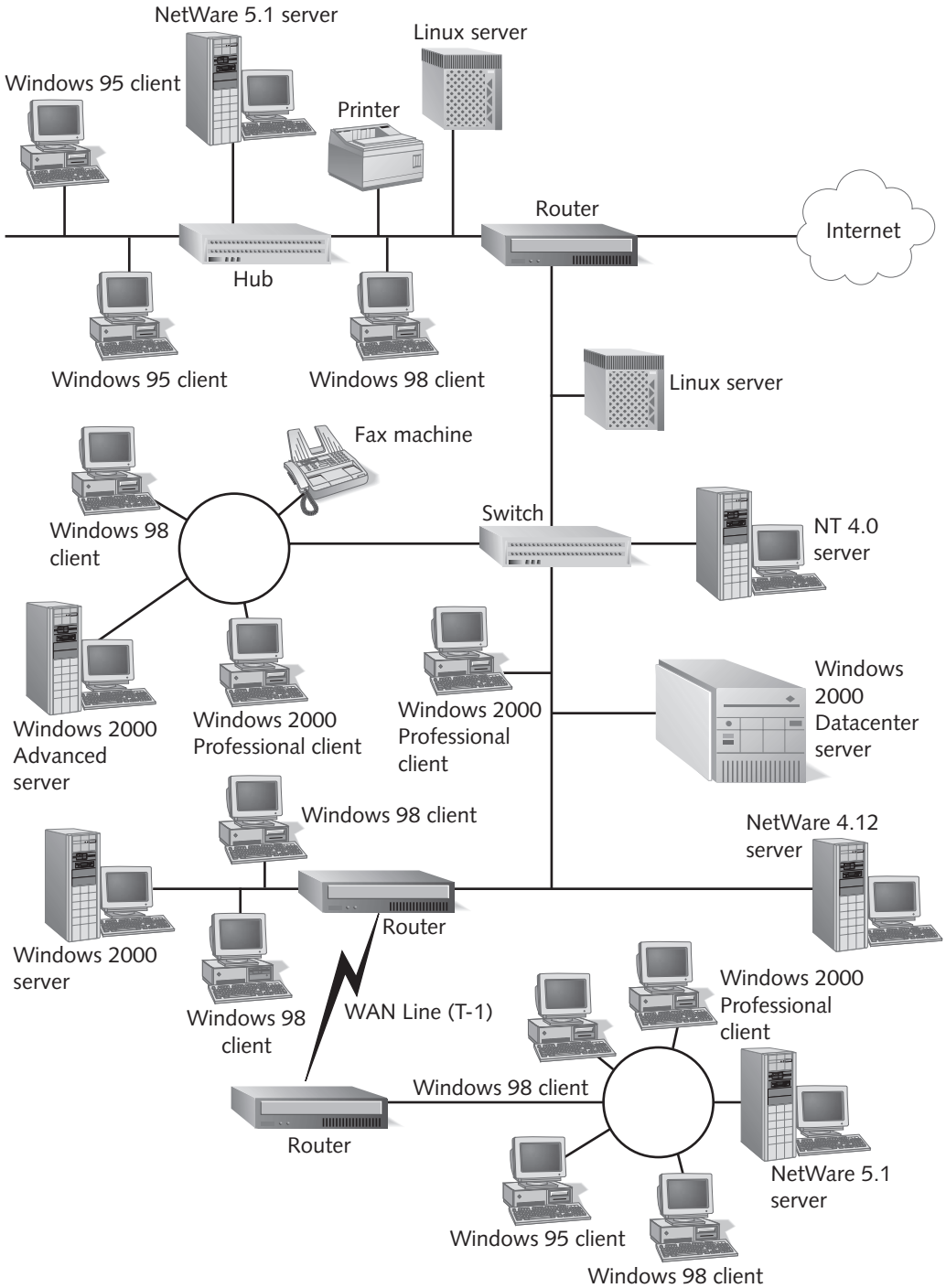

Figure 2-1 A mixed environment utilizes multiple operating systems

Sometimes an organization utilizes multiple operating systems because of a gradual evolution within the company. Perhaps the organization started out with UNIX application servers and Windows 95 workstations, but later added Novell NetWare file and print servers for users to store and print files. (**UNIX** usually operates on more expensive RISC-based processors. **Linux** is a version of UNIX and operates on PCs in addition to Alpha RISC-based processors and PowerPC processors.) The expensive UNIX hardware platform became less attractive compared to a less expensive PC computing platform, so PC servers running Windows NT 4.0 and Linux were added. Later, the organization upgraded client computers to Windows 2000 Professional and the UNIX hardware platform to PC servers running Linux. Regardless of the path an organization takes to arrive at its current constellation of operating systems, the network administrator must ensure that all operating systems interoperate as seamlessly as possible.

Operating system vendors have come to realize that no one operating system will meet every need, and they have produced various patches and other software to allow interoperability. For example, a Windows NT 4.0 logon server and a NetWare file and print server may have to interoperate. In this case, you probably want users to log on to the Windows NT 4.0 server as usual and access files on the NetWare server. Users should not be required to log on to the NetWare server separately if you want seamless interoperability. Instead, users access resources on the file and print server without any awareness that it is a NetWare server. Microsoft includes Gateway Services for NetWare with Windows NT 4.0 (see Figure 2-2). This product allows users to access NetWare resources through the Windows NT 4.0 computer. Whatever network environment you find yourself in, research the various operating system combinations and find the resources that allow the best interoperability.

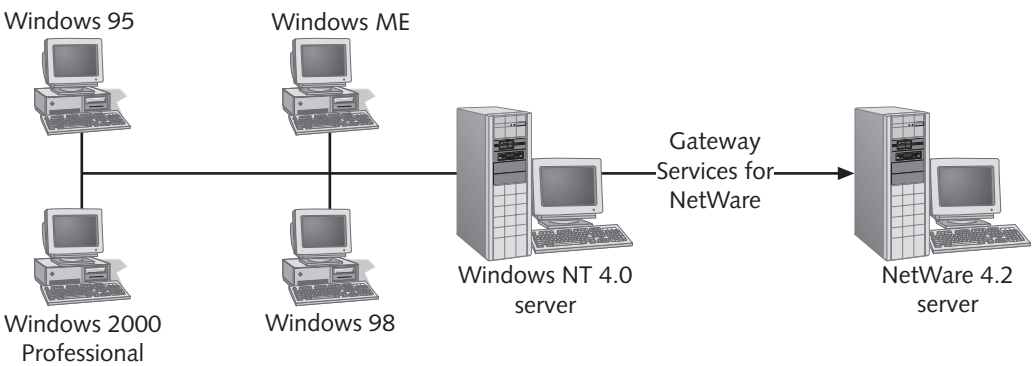

Figure 2-2 Gateway Services for NetWare allows access to the NetWare server

Consider protocol incompatibilities in the mixed environment as well. Continuing the previous interoperability scenario involving Windows NT 4.0 and NetWare, realize that Windows NT 4.0 installs TCP/IP by default, and NetWare often uses IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange). These two protocols are

incompatible. For interoperability purposes, you would probably install both TCP/IP and IPX/SPX on the Windows NT 4.0 server. Then, the Windows NT 4.0 server can internally translate from IPX/SPX to TCP/IP (and vice versa) as messages travel to and from the NetWare server (Figure 2-3).

Adding Gateway Services for NetWare automatically installs IPX/SPX on the Windows NT 4.0 server.

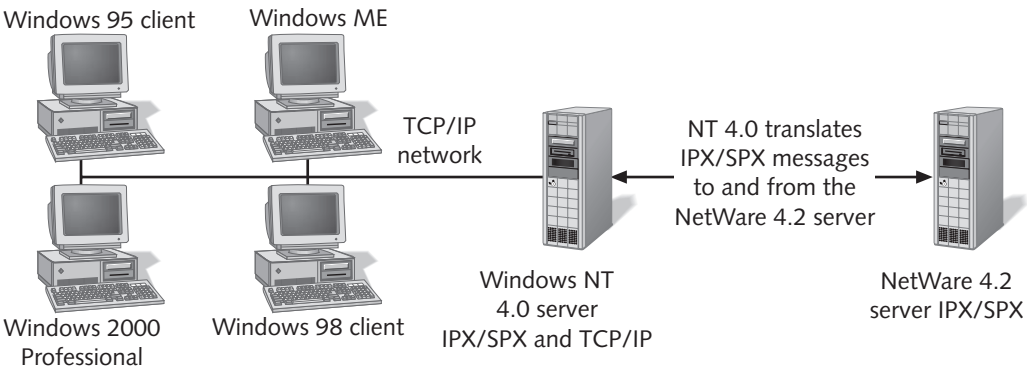

Figure 2-3 Using TCP/IP and IPX/SPX, Windows NT 4.0 can communicate in both protocols

Prior to adding another operating system to your network design, be sure to test for possible incompatibilities. For example, perhaps your UNIX system uses a custom-designed database. If you plan to install Windows 2000 Server, it will not be able to use the same application. You will either choose a different database product or pay to port the application to the Windows platform.

Also consider the interoperability of network operating systems with client workstation operating systems. For example, if you install a NetWare server in a LAN that uses Windows 98 computers, can the Windows 98 computers access all the benefits of the NetWare server? In fact, they cannot do so using the Microsoft Client for NetWare Networks software that is included with Windows 98. In order to utilize the powerful features of Novell Directory Services (NDS), Windows 98 clients must download and install the Novell Client v3.3 for Windows 95/98 from Novell (Figure 2-4). (**Novell Directory Services (NDS)** is an example of a directory service, a hierarchical database of network resources that allows users from anywhere in the enterprise to access resources throughout the organization. Microsoft Active Directory is another example of a directory service.) An **enterprise** is a geographically dispersed network under the jurisdiction of one organization. It often includes several different types of networks and computer systems from different vendors.

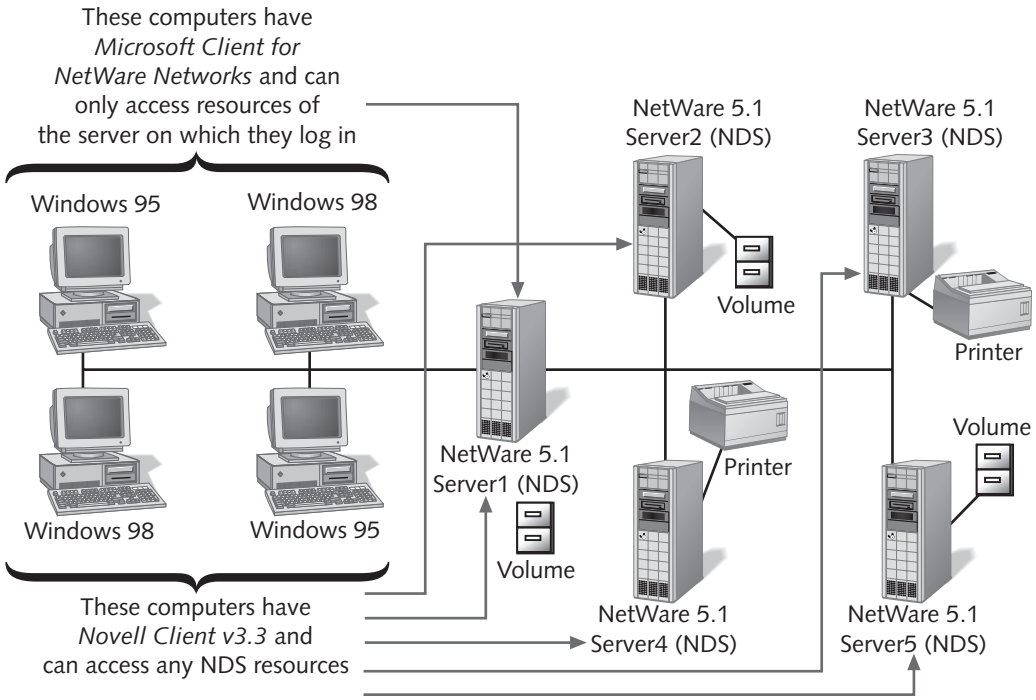

Figure 2-4 Novell Client v3.3 for Windows 95/98 allows access to NDS

TIP

You might also consider using the NDS Authentication Services (NDS-AS) 3.0 download from Novell to allow users to log on to NDS transparent from virtually any other operating system platform. NDS-AS transparently redirects the user credentials to the NDS database for authentication and authorization. Other vendors also use credential redirection, known as a **single sign-on**.

Caution

If you decide to convert from one NOS to another, be aware that the user and group accounts are incompatible between operating systems. For example, if you want to convert from NetWare to Windows NT, the NetWare accounts are not readable by the Windows NT operating system. However, most NOS vendors offer a migration tool that allows you to separately convert the accounts.

Server Placement

No matter how good your business sense, ability to meet user demands, or skills in server interoperability, a service outage and lengthy recovery significantly impact the business of the organization. One of the most critical issues in server planning is assessing the physical location at which you plan to install the servers. An improper server environment can result in severe problems later on. Installing a server involves much more than

finding an empty space, plugging it in, and installing the operating system. You must also place the server so that it serves network users in the best possible way. In a global enterprise, also consider factors such as site links and bandwidth utilization within and between networks.

For example, you might be from the United States and accustomed to reliable, high-speed WAN links. However, many locales have slower or less reliable connections. A WAN link connects a **site**, which consist of the LAN(s) on either side of a WAN connection. Figure 2-5 illustrates a WAN with two sites and two site links.

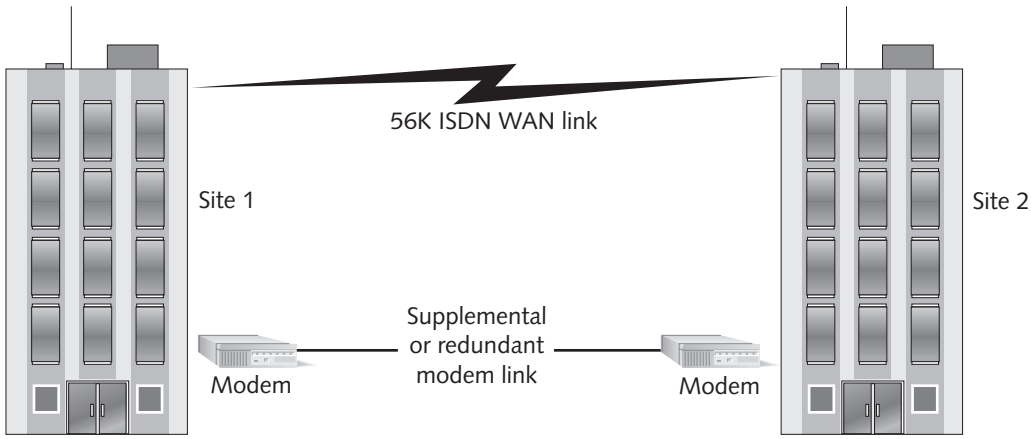

Figure 2-5 Two sites utilize a WAN link and a modem link

If the WAN link is slow but is the fastest type available in that locale, consider adding an additional WAN link of the same type. For example, the best available connection at some locations might be a 56 Kbps ISDN (Integrated Services Digital Network) from the telephone company. The advantage of an ISDN connection is that you can either leave it in an always-on state or have it dial out to another site on demand (which is useful if the telco charges for connection time). Also, an ISDN line usually provides clean, consistent data transmission. If this single connection is too slow, you might be able to combine two ISDN channels and double the speed, or add a dial-up modem connection to increase bandwidth during peak times (again refer to Figure 2-5). The dial-up connection can also provide redundancy in case the ISDN line fails.

Server placement within your WAN has an impact on network service and response to user requests. First, let's look at server placement within a site, and then at server placement for connecting sites.

Intra-Site Server Placement

Intra-site communication refers to communication between hosts within a single site, often over a LAN. Within the site, you should determine the best location in the building and on the network to place the server. Even a high-powered server's performance can flounder if the server is poorly placed. Although most network connections in a LAN are high-speed and well-connected, you should still carefully place the server in the most efficient location possible. Most networks represent a progression of growth both technologically and physically over a period of years. As a result, a network might have some locations that offer better connectivity than others. Figure 2-6 shows a network that originally started with a 4 Mbps network. As the network grew, a new section utilized a 10 Mbps network. Later, a 100 Mbps section was added. However, the servers remain in the 4 Mbps section.

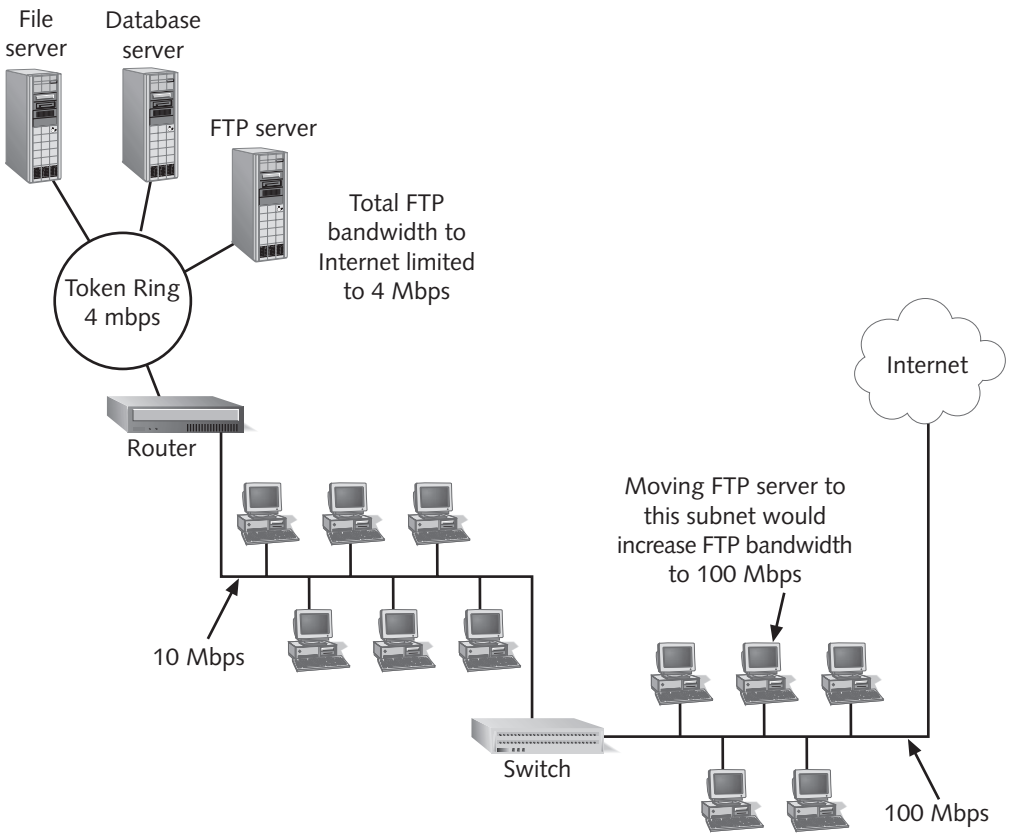

Figure 2-6 A network with various bandwidth speeds

Users on the 4 Mbps network seldom complain of bandwidth speed connecting to the servers because they have never experienced speeds faster than 4 Mbps. Users on the 10 Mbps network complain more often, and users on the 100 Mbps network complain

every day about slow service from the servers because those users can compare 10 or 100 Mbps speed to 4 Mbps speed. The connection speed problem compounds with outside sources accessing the servers. For example, if one of the 4 Mbps servers were a **File Transfer Protocol (FTP)** server, the effectiveness of the server file transfer would be severely limited. It would be better to move the servers from the 4 Mbps network to a faster section, or to redesign the network so that all sections are at 100 Mbps.

Though these seem like simple solutions, in some environments making these changes could be a difficult task for several reasons. Perhaps the 4 Mbps network is large, and it requires a significant equipment investment to upgrade all equipment, including hubs and the NICs, on all servers and clients. Even if it were impractical to upgrade the 4 Mbps network, you would still want to move the servers. Moving a server might also prove to be problematic if the higher-speed networks do not have the physical facilities necessary for such a move—such as if a server room or closet were not available. If servers were added to the 10 or 100 Mbps networks that replicate data with servers on the 4 Mbps network, then the 4 Mbps network would experience even higher bandwidth utilization, limiting the effective shared connection speed for all other network hosts.

A 4 Mbps network is typical of earlier Token Ring networks; 10 Mbps and 100 Mbps networks are typical of current Ethernet networks.

Inter-Site Server Placement

Inter-site communication refers to communication between hosts in different sites, often over a WAN link. Servers communicating over a WAN link also require you to determine the best connection method to optimize your bandwidth. When planning inter-site network communication across a WAN, you should generally place the servers that directly communicate across the WAN in closest physical and logical proximity to the WAN link. This makes sense because it reduces the number of variables between the WAN link and the server. In addition, placing the server as close as possible to the WAN link helps ensure that the server receives the maximum available bandwidth from the WAN.

If you place the server further away from the WAN link, you increase the number of possible problems. For example, additional hubs, switches, or **routers** (network devices that divide the network into separate parts usually known as **subnets** and forward network traffic to appropriate destinations) each add a potential point of failure in the data path between the WAN and the server. For example, in Figure 2-7 a Windows NT 4.0 domain controller is moved closer to the actual WAN connection, removing potential intermediate points of failure. Also, placing the server further away from the WAN link slows down network performance, because data traveling from the WAN must compete with other network traffic that occurs within the LAN.

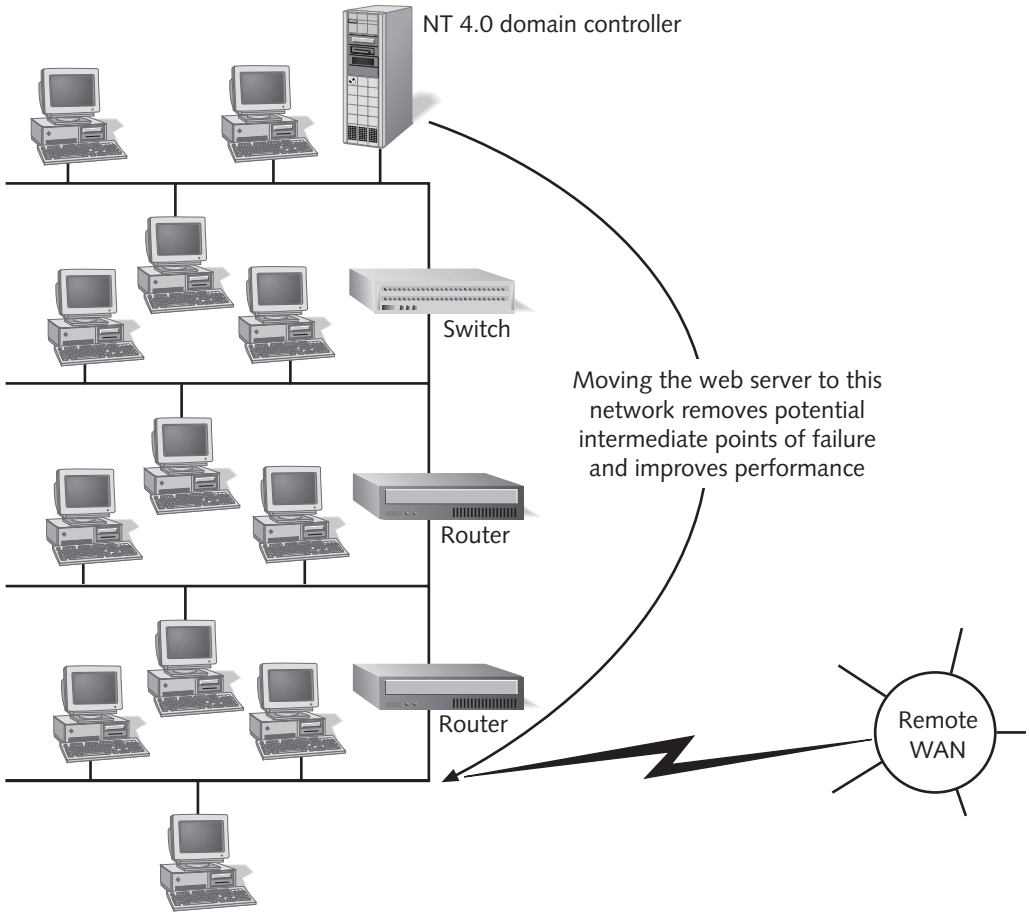

Figure 2-7 Inter-site server placement can improve availability and performance

Creating the Network Diagram

A network diagram is a physical and/or logical representation of the network, and is also known as a network map. You create a network diagram to design a network, keep a record of the network, or assist in changing or troubleshooting a network. You can draw a network map by hand, but regardless of your artistic skills, you should use special software designed to create a network diagram (see Figure 2-8). As a technician, you will find it much easier to trace problems if you have a diagram of what the network looks like. For example, if you visit a large network and you have little knowledge of its physical or topological structure, attempting to physically locate a failed server might be difficult without a network diagram.

The network diagram also provides a record and justification for why an organization decided to use specific servers, why the servers are placed in their specific location, and helps to logically determine a course of action in making a change to the network design and in troubleshooting.

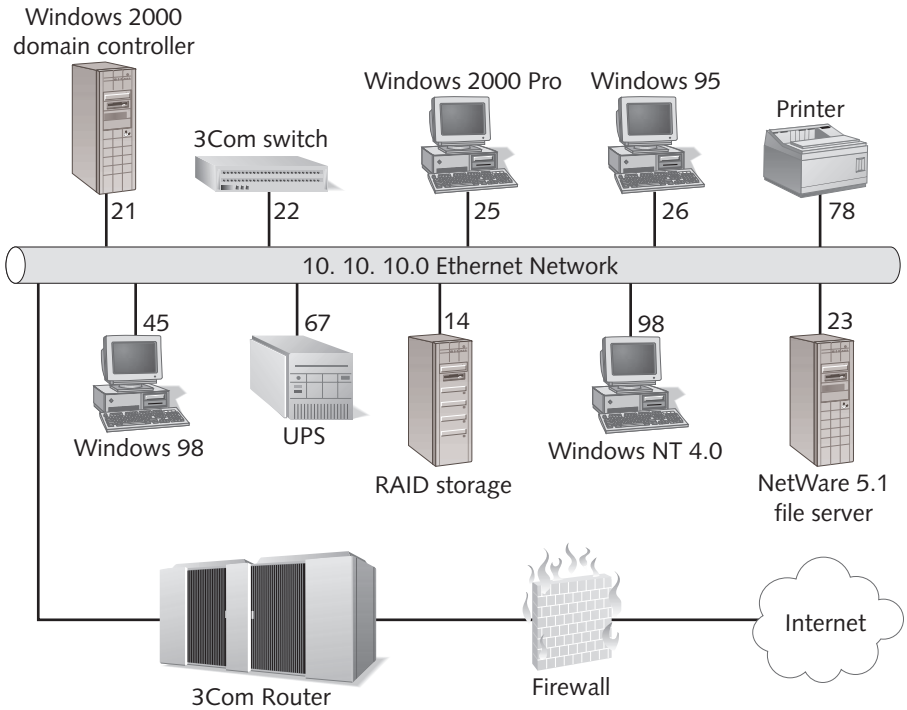

Figure 2-8 Network diagram (Visio)

Many companies use programs such as Visio 2000 to create network diagrams. Visio 2000 includes several predrawn images of various types of computers and network equipment. Using drag and drop, you can whip up a dream network in no time. If the network design changes, you can drag and drop the changes directly on the diagram and the rest of the network adjusts accordingly.

Planning Physical Site Readiness

The physical server environment is one of the most critical aspects in determining where to place servers. In fact, you might have to significantly modify a particular room to ensure that the conditions are optimal for server reliability and uptime. Variances in the physical environment can also affect the lifetime of the server and its components. The two most significant factors affecting the health of a server are temperature and humidity. Other elements about the site's physical readiness include floor space, power availability, and the possibility of a fire or flood.

The physical site plan for your server room is foundational to the success of your network. However, you cannot plan a new server room yourself, regardless of how much you know about servers and networking. Several key planning considerations require the involvement

of an architect, electrical and mechanical engineers, and a general contractor. For example, you probably do not want to design a fire suppression system on your own. For that, you would use a mechanical engineer to ensure the best possible solution for your environment and to avoid liability on your part and that of your organization. Also, these professionals can ensure that the server room installation complies with federal OSHA requirements and local building codes.

Temperature

Servers run hot. When you consider individual factors that contribute to the server heating and put them all into a single box, temperature problems quickly compound themselves. The hottest element is and will probably always be the processor(s) (Figure 2-9). The processor consists of around 40 million tiny transistors, each charged with electricity, albeit a small amount at about 1.7–3.5 volts. (A **transistor** is an electronic device that opens or closes, or turns on or off to provide a logic gate or switch, and provides the "thinking" capability of the processor.) Maximum temperature tolerance for the processor is about 185° Fahrenheit (85° Celsius); however, you should never allow the temperature to get this high. Fans and other cooling measures dedicated to the processor help to keep the temperature at 90–110° F (32–44° C). If you have an SMP system with multiple processors, potential temperature problems multiply accordingly.

Other hot components in the system are the hard drives, which on a server often have cooling fans of their own, and the motherboard. Internal components in the server collectively contribute to the overall heat of the server room. The increased heat in the air results in warmer air entering the server and aggravates the heat issue, which is why the server room should have dedicated air conditioning.

Figure 2-9 Processors can be very hot; cool processors to 90–110ºF (32–44ºC)

Generally, a series of fans inside the case helps keep the system cool and achieves maximum effectiveness if the ambient (i.e., surrounding) room temperature is also cool. In order to provide cool ambient temperature, keep the air conditioning in the server room as cool as possible. To compromise between human comfort and cooling server equipment, you can usually keep the server room temperature between 68 and 72° F (20–22° C). However, be sure to keep the temperature at a constant setting, because temperature fluctuations cause expansion and contraction of server components, shortening the server's life span.

Because equipment in the server room generates heat disproportionate to the heat level in the rest of the office, setting a thermostat in general areas cannot adequately cool the server room. A thermostat set at 70° F (21° C) for general areas will allow significantly higher temperatures in the server room. Therefore, it is important to provide an independent air-conditioning system and thermostat in the server room. If the budget allows, also consider installing two air-conditioning units and thermostats in the same server space for redundancy (Figure 2-10). If one unit fails, the other should be able to cool the room.

Unless the site is in an extremely cold natural environment, you will seldom need to provide heat to the server room—it provides plenty of heat on its own.

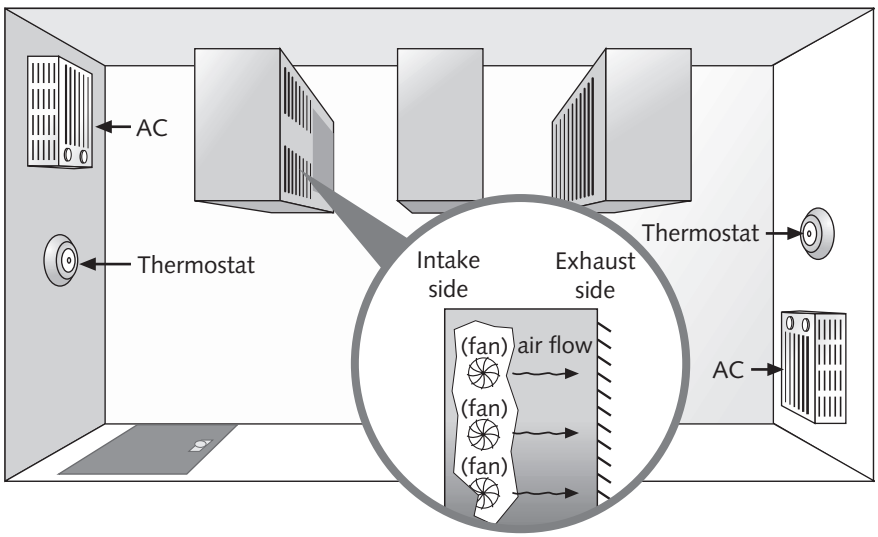

Figure 2-10 Use separate thermostats and air conditioners in addition to internal equipment fans to cool equipment

Regardless of the ambient room temperature and adequacy of server cooling fans, the server cannot adequately cool itself unless you provide good airflow to the server. This is an often-overlooked factor for a number of reasons. For example, server rooms often

lack adequate space. As administrators cram more equipment into the server room, they are often forced to shove equipment closer to the wall to create more usable floor space. Or, someone receives a new carton of equipment and, for lack of a better place, simply places it in front of the server rack—unaware of the fact that he or she has just blocked the ventilation slots to the server. Space in front of and behind the server or server rack is critical. According to most specifications, about three feet of clearance is required both in front of and behind the rack (Figure 2-11).

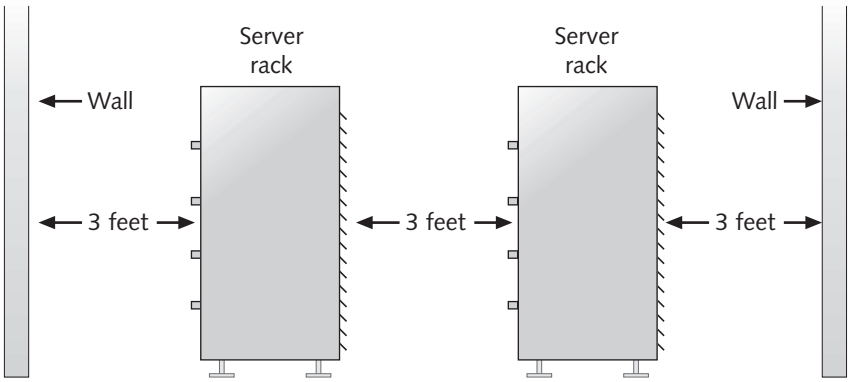

Figure 2-11 Allow three feet in front of and behind server equipment

Air Quality

While air quality sounds like a health-related issue for people, it is also an important issue for server equipment. Air quality in a server context means that the air must be clean and as free as possible from dust particles. Rooms designed to house server equipment often have added filtration beyond the usual air filters installed in the general-purpose HVAC (heating, ventilation, and air conditioning) system.

Excessive dust in the air directly relates to the previously discussed issue of temperature. A layer of dust effectively becomes insulation on server components. Insulation is fine for a home, where you want to keep heat inside, but it's *not* fine on server components, where you want to prevent heat as much as possible. Also, dust particles can adversely affect moving parts such as floppy and hard disks. Dust accumulation can also present a fire hazard. Take regular measures to clean dust off of all server components, regardless of air cleanliness. Add supplemental air filtration to any server room that does not already have it.

Remember that dust begets more dust. Passersby or air movement from the HVAC system easily disturbs a layer of dust. While you as the administrator are responsible for maintaining dust-free components, a cleaning service can remove dust in general areas. There are contractors who specialize in cleaning controlled environments, such as your server room, using highly trained crews. An example is Data Clean Corporation (see Hands-on Project 2-4).

Contact any reputable commercial HVAC or mechanical company to assess the air quality in your server room and make recommendations. Many organizations are large enough to require their own on-site facilities engineers, who might also be a good source of information on air filtration.

Several server components—such as the power supply fans, supplemental cooling fans, server racks and cabinets, and hard disks—might also include supplemental filters. For example, a force-filtered server uses one or more filtered fans to supply main internal airflow throughout the server. Other cooling fans inside the server only draw upon this filtered air, creating a **positive pressure** environment (Figure 2-12). In server rooms that are extremely sensitive to dust, you can also install an adhesive pad in front of the server room door that collects dust particles from the bottom of shoes as people enter the room.

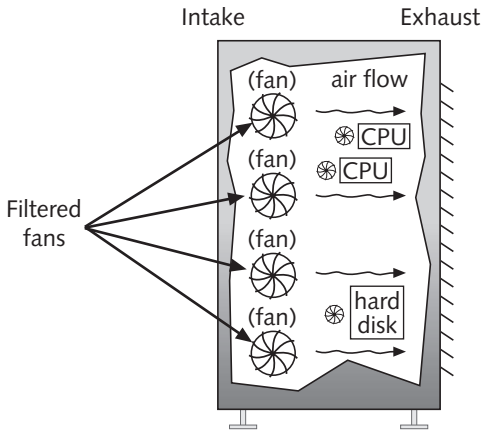

Figure 2-12 A positive pressure environment helps ensure clean air inside the server

Humidity

Humidity factors vary widely depending upon the physical location of the site. For example, the desert climate of Phoenix is not as likely to present the same humidity issues as the rain-soaked climate of Seattle. Humidity affects the health of electronic server components because a drier environment presents a greater occurrence of electrostatic discharge. **Electrostatic discharge (ESD)** is static electricity that can damage, destroy, or shorten the life of the server's electrical components. Many servers specify operating allowances between 20 percent and 80 percent **noncondensing relative humidity** (noncondensing means there is no moisture accumulation, such as on the outside of a cold glass). However, you should strive to humidify or dehumidify the air as needed to keep the humidity range between 40 percent and 60 percent.

High humidity presents the possible problem of condensation on equipment, which could obviously drip onto electronic components and generate significant damage—not to mention an electrocution and fire hazard to personnel. Even high-humidity environments do not normally cause condensation unless the temperature changes drastically—perhaps due to an HVAC outage. Higher humidity can create corrosion on metal components such as adapter cards and memory chips, and accelerate deterioration of magnetic media such as tape backups and floppy disks. Few environments contend with high humidity because both heating and air conditioning automatically remove humidity. However, you might find higher levels of humidity in basements or other subterranean locations, or environments that do not have a quality HVAC system in place.

If humidity is too high or too low, HVAC companies can offer a variety of solutions to add or remove humidity. Typically, HVAC modifications add humidity to the air that flows from the heating or air-conditioning unit. Utilize a dehumidification solution from the HVAC company as well. For economic reasons, you might be tempted to utilize a household dehumidifier in smaller server rooms. However, I cannot recommend these units for at least two reasons. First, these units are designed to cycle on and start dehumidifying based on a humidity threshold setting. When the unit powers on, it might cause a brief dip in power level if it is on the same circuit as server equipment (more on power later in this chapter). Second, these units usually remove the humidity from the air by condensing it into water in a pan. The pan must be emptied regularly—an overflowing pan threatens safety (slick floors) in addition to electrical hazards.

Look for equipment manufacturers that specialize in equipment that addresses the special air-conditioning, filtration, and humidity requirements of a server room (try Hands-on Project 2-5). Figure 2-13 shows a self-contained Liebert air-conditioning system that fits nicely into the corner of an existing server room, and filters air for dust control.

Figure 2-13 An air conditioning unit controls temperature, humidity, and dust (*www.liebert.com*)

Flooring

In a server room, flooring is much more than a location on which to place equipment. Flooring can have a direct effect on the health of your servers, particularly in respect to the risk of ESD and the efficiency of cooling. In practical terms, flooring also affects where you put cable and smoke alarms. Choose from either a flat floor or a raised floor—each has its own characteristics and advantages.

A flat floor usually involves commercial-grade floor tiles on top of concrete. Check with your architect for floor tiles that can withstand the pressure of heavy server

equipment and are static-resistant. Inevitably, some equipment will scar or crack tiles, which is not a functional issue if the damage is only cosmetic. To plan for future equipment additions and rearrangements in the server room, be sure to request extra replacement tile. Also consider no-wax flooring to avoid the time-consuming and messy job of stripping and applying wax, in addition to the regular maintenance of machine buffing, which can generate a flurry of dust. Avoid carpet because it can retain dust and presents a static risk despite manufacturers' best efforts to make static-resistant carpet.

A flat floor requires you to place cable, power lines, and HVAC ducts inside walls and above ceiling tiles between the actual ceiling and the dropped ceiling—a space known as the **plenum** (Figure 2-14). Running cable in the plenum might not always be possible (for example, in an older building that does not have a plenum area).

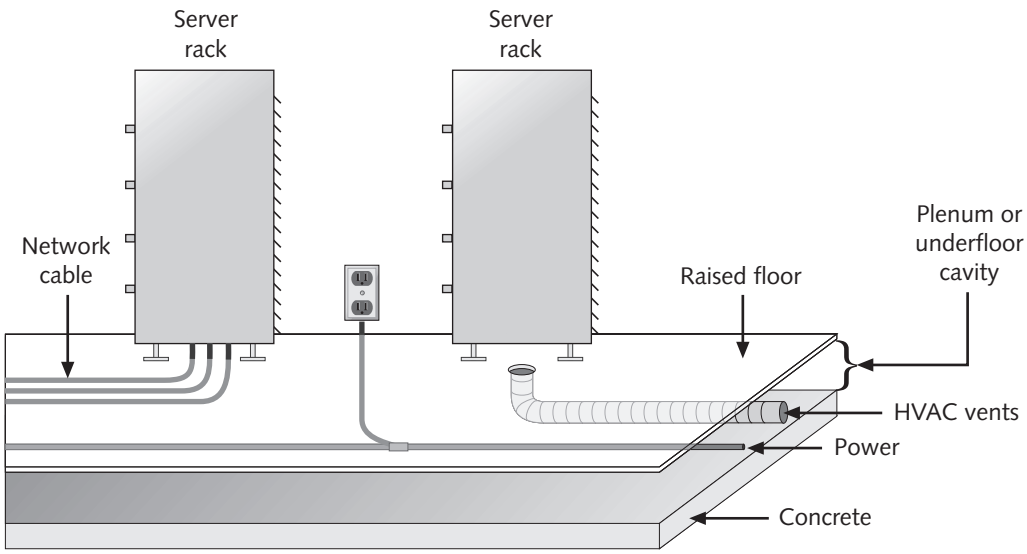

Figure 2-14 The plenum is useful for cable runs HVAC vents, and power lines

A raised floor attaches to supports that provide a subfloor between the concrete floor and the floor panels (see Figure 2-15). This space (also called a plenum or under-floor cavity) serves the same purpose as the plenum in the ceiling—you can run cables, power lines, and HVAC vents in this space.

Gasses and smoke emitted by burning cable can be noxious, so in both the plenum and subfloor, you must use plenum-rated cable (coated with a Teflon-like material) to limit the spread of flame and smoke.

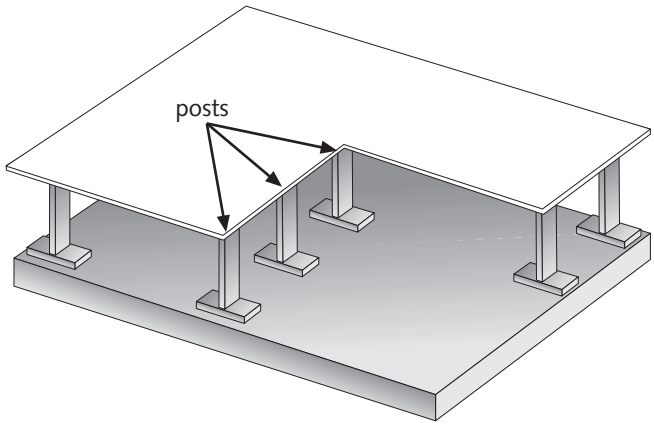

Figure 2-15 A raised floor rests on posts and provides plenum space

The depth of the subfloor varies from one design to another, but it usually involves 2-foot-by-2-foot panels 11 inches above the concrete. (You can adjust the height using different sized supports.) Raised floor installations were quite common in the era of large mainframes, and then became less common as more compact PC-based servers played a larger role. Server rooms became smaller as organizations decentralized from a very large room containing all servers to multiple smaller server rooms. Now, many organizations use a datacenter to house space-consuming equipment or consolidate contents of departmental server closets into a single, centralized, larger server room. (**Datacenter** is a term with two meanings, depending upon the context. It can refer to a consolidation of the majority of computer systems and data into a main location, or it can refer to one or more very powerful servers optimized as database servers—sometimes configured with as many as 32 processors. This context references the former.)

Heavy-duty floor panels are designed to withstand an enormous amount of weight (over 1000 lbs each) and are often steel filled. Some floors use an I-beam construction for added stability at the edges of the panel. These panels can be very heavy, weighing up to 45 lbs each, and require a floor puller with suction cups to lift them off the supports (Figure 2-16). The floor surface is specially coated to reduce ESD.

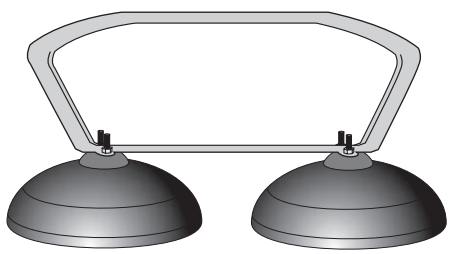

Figure 2-16 A floor puller uses suction cups to remove floor panels

When running cable in either the ceiling or floor plenum, consider using cable trays or other cable organizers to prevent a tangled mess and minimize future troubleshooting efforts. Also consider pulling the cable through a conduit to minimize interference with other mechanical equipment and to make replacing cable more feasible should the need arise.

Raised floors (Figure 2-17) offer excellent grounding to avoid ESD. Many designs ground each supporting post and offer grounding points for server racks, cabinets, or other equipment. You can place HVAC vents beneath cabinets or racks to force cooled air up through the equipment. A cabinet usually includes at least one 10-inch (25.5-cm) fan (and several supplemental fans) at the top to draw cool air through the opening at the bottom and expel warm air at the top.

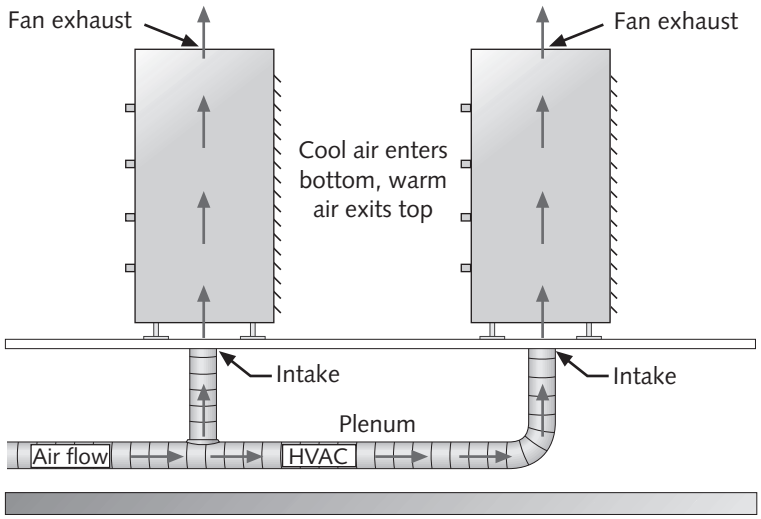

Figure 2-17 Raised floors can assist the cooling of server cabinets and racks

In a flat floor environment, the cooling system can be reversed. You might place the rack or cabinet directly beneath a cooling vent so that cool air enters through the top and warm air exits through the bottom.

Coordinate raised floor installations with your architects, engineers, and general contractors. Raised floor materials are available from many vendors. For a good start on the physical installation of raised floors and server rooms in general, visit the following web sites:

- *www.beanfield.com*
- *www.accessfloorsystems.com*
- *www.compucraftconstruction.com*

As a safety precaution, place highly visible signs in areas where you remove a tile to access the subfloor, as shown in Figure 2-18.

Figure 2-18 Warn others of an open floor

POWER

Designing an appropriate power solution for the server room is one of the trickiest considerations and should fall almost completely to the electrical engineers. Just tell the engineers what you want and the level of redundancy you require, and depend upon them to provide the solution. When providing planning objectives to the engineers, be sure to consider the factors of availability, quality, and susceptibility to electromagnetic interference.

Availability

Three power sources provide power to the server room: the main power supply, the uninterruptible power supply (UPS) for temporary power, and backup generator power for extended, system-wide outages. Make sure to request dedicated circuits to the server room that are separate from the building's main power supply. Calculate the total power the current equipment requires, including servers, monitors, routers, hubs, and switches. Add to this calculation anticipated amperage requirements for future expansion, and ask the electrical engineers to oversupply the power requirements just to be sure. (Also make sure to install plenty of easy-to-reach electrical outlets.)

Although you should rely on an electrical engineer to design server room power, you might also want to keep on hand the IEEE (Institute of Electrical and Electronic Engineers) publication *IEEE Recommended Practice for Powering and Grounding Sensitive Electronic Equipment* (ISBN 0-7381-1660-2). This book is also known as the "emerald book" in reference to its cover color, and provides complex electrical information such as reducing electrical noise and ensuring proper grounding. You might find it hard to locate in retail stores, but you can obtain it from *www.ieee.org*.

Administrators can probably determine what kind of UPS to use; however, the engineer should plan main power and backup generator power. The purpose of the UPS and backup generator is to provide redundancy, ensuring that power is available at all times. The UPS (more details in Chapter 3) supplies power temporarily while administrators perform a graceful shutdown of server equipment. Otherwise, the sudden loss of power to the server can be extremely damaging to the operating system, applications, and open data files. Figure 2-19 shows a typical power configuration for a server room.

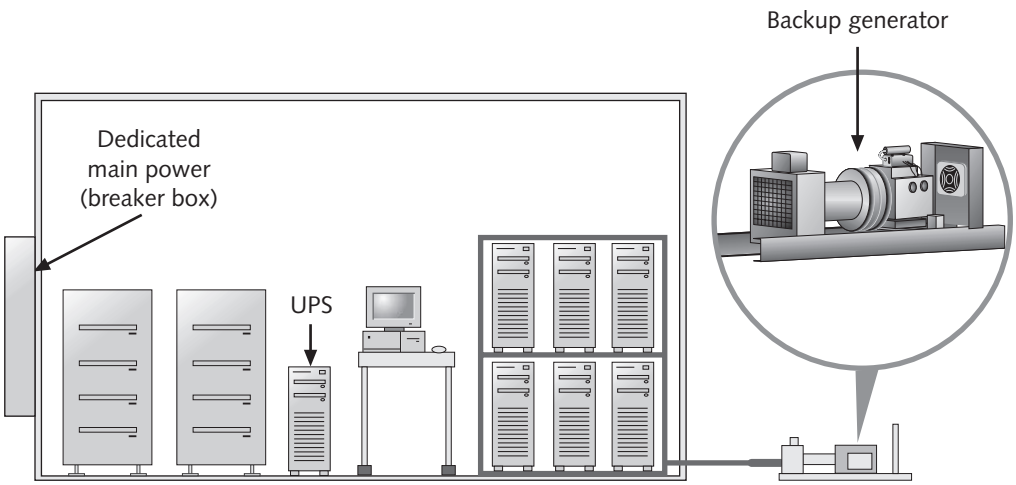

Figure 2-19 Main power, UPS systems, and backup generator provide power to the server room

Backup generators can be extremely expensive depending upon the amount of power they provide. Some generators cost about $250,000 and require a facility of their own, separate from the main building. Backup generators operate for as long as diesel fuel or natural gas is available. You will still need UPS systems because it usually takes about 15 seconds for the generator to start up and supply power. Of course, only organizations that absolutely require 24/7 operation would opt for such an expensive generator, which might also provide main power to the rest of the organization.

Make sure to request a "phase protector" in the backup generator system. Otherwise, the backup generator might confuse the UPS, causing it to continue to supply and eventually drain battery power.

Quality

Clean power extends the life of the server and its components. "Clean power" means the absence of surges, spikes, dips, or poor grounding, which can lead to short circuits, tripped electrical breakers, and possibly damage to equipment or people. Use a receptacle tester (also known as a polarity tester, Figure 2-20) to test receptacles for power and grounding, especially in older buildings that might have questionable electrical wiring.

Figure 2-20 The receptacle tester verifies power and ground wiring

Request that the electrical engineer provide a connection to the earth ground in the server room. The earth ground of a home typically connects to the plumbing outside that provides water into the home. In a commercial building, electrical engineers usually design the earth ground to utilize a rod that is driven deep into the ground (Figure 2-21).

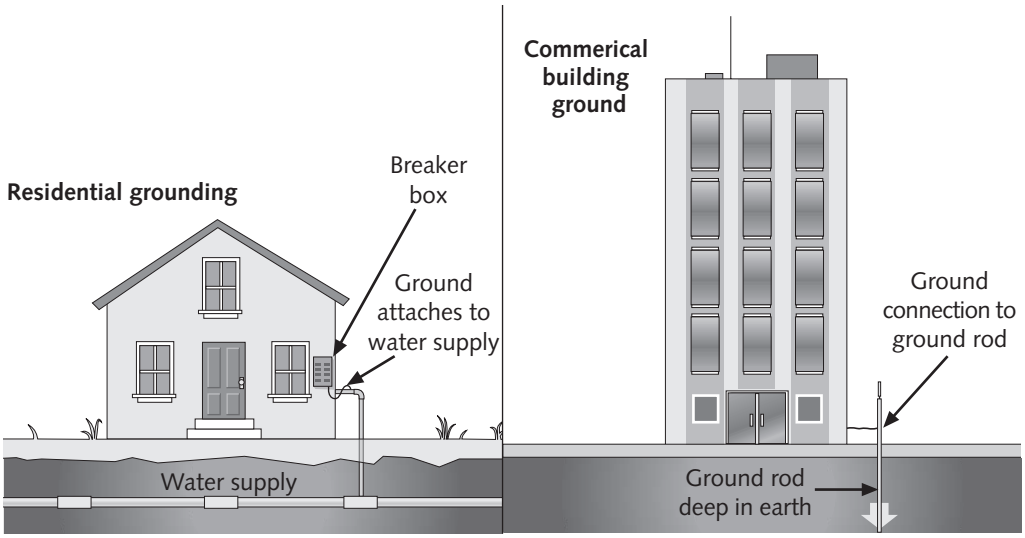

Figure 2-21 A commercial earth ground is a rod forced deep into the earth

The electrical engineer takes measures to ensure clean power, but the administrator also ensures clean power to the server by using good surge protectors, UPS systems, and possibly line conditioners, which supplement power in the event of a brownout and/or minimize electromagnetic interference (EMI).

Electromagnetic Interference

EMI is a byproduct of electricity and can disrupt or corrupt data traveling along network cable as well as disrupt other electrical equipment. Design data cable routes to and from the server room so that they avoid electrical equipment such as fluorescent lights, heavy electrical equipment, motors, and so forth. Make sure your electrical engineer is aware of the types of other equipment (such as heavy manufacturing equipment) in your organization so that he or she can design around potential EMI pitfalls. Shielded twisted-pair (STP) network cable includes a foil inner jacket, adding a level of protection against EMI (Figure 2-22); however, you should avoid EMI sources when possible.

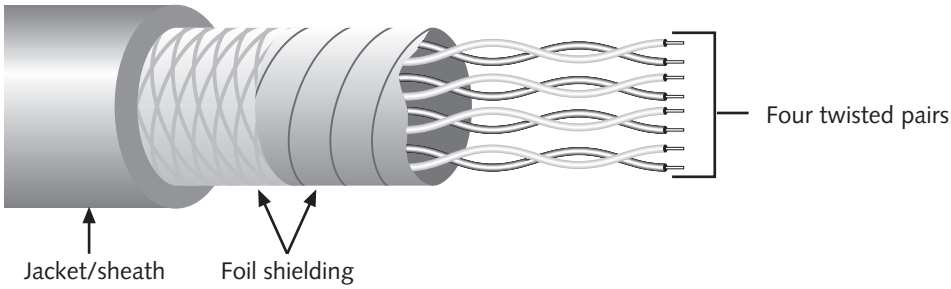

Figure 2-22 STP cable includes a foil inner jacket to protect against EMI

Because servers and associated equipment are electrical devices, they also produce a level of EMI. While most equipment manufacturers take precautions to minimize the production of EMI, a certain level is unavoidable. If you find that certain server equipment exhibits strange, intermittent problems that do not seem to be associated with a specific component or the NOS, try moving the equipment to a different location where there might be less EMI from surrounding equipment. Also be sure to cover any open drive bays and expansion slots, and leave covers attached to servers when you are not servicing them. Otherwise, these exposures can radiate EMI.

If a situation arises in which you need to shut off a breaker, the description next to the breakers might be blank, incomplete, vague, or just plain wrong. Verify that you are about to switch off the correct breaker so that you do not inadvertently shut down other systems. You can use a circuit breaker finder, which is actually two pieces. The first piece (the transmitter) plugs into an electrical outlet on the circuit you wish to shut off (see Figure 2-23a). The second piece (the receiver) emits a tone when you physically pass it over the correct breaker (see Figure 2-23b).

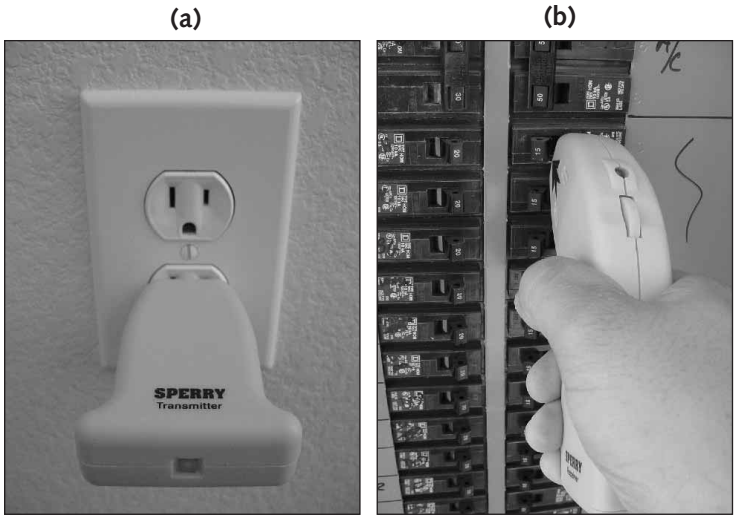

Figure 2-23 The circuit breaker finder locates the correct circuit breaker

Disaster Planning

Disaster planning requires a significant budgetary outlay for the relatively unlikely possibility that a natural disaster, building defect, or other unexpected occurrence takes place. However, in the event that a disaster does occur, you will be glad for every penny spent in planning. Much of this book teaches disaster planning in various respects, such as the typical hard disk failure; however, this chapter focuses on planning the server room to be as resilient as possible in case of fire or flood.

Fire Detection and Suppression

A fire presents an obvious threat to people and equipment. Most buildings are built (or remodeled) according to relatively stringent OSHA regulations and local building codes. As a result, people sometimes dismiss the threat of a fire. However, alert administrators must remain keenly aware of the possibility of a fire (particularly an electrical fire) in both planning and daily operations. If there is a single location at which a fire is most likely, it is probably a single room filled with complex electrical equipment. That's right—the server room.

First, in the event of a developing fire, you must ensure that people in the server room are notified of the danger. Smoke alarms serve this purpose, and commercially available alarms can alert emergency services and people within the organization in addition to setting off an audible alarm. While most smoke detectors are in the ceiling, they can also

be in the subfloor in a raised floor design. If they are in the subfloor, you should mark the surface of the floor panel above the smoke detector with adhesive signs, so that if it goes off you can more easily find it when it's time to reset or maintain it.

In years past, halon was the primary fire suppressant in server rooms because water has an obvious negative impact on electronics. Essentially, a fire is a chemical chain reaction. Halon breaks the chain reaction by substituting hydrogen atoms with halogen atoms. Halon leaves little or no residue and does not cause electrical short circuits. However, some suspect that halon can cause corrosion on computer components. Because halon is harmful to the earth's ozone layer, the Environmental Protection Agency (EPA) has banned the production of new halon, although you can purchase recycled halon. Because halon is being phased out, you might want to choose a different chemical fire suppressant. Consult EPA's list of halon substitutes at *www.epa.gov/ozone/title6/snap/halonreps.html*. Unfortunately, converting to another fire-protection chemical involves more than replacing the gas canisters—you must replace the entire system. Whatever product you use to extinguish fire, consider that you might also need an emergency ventilation system to expel gasses from the suppressing chemicals or burnt objects.

If you choose to supplement the chemical extinguisher, consider using a dry system instead of a water sprinkling system. A dry system uses water but only fills the pipes when there is a fire, ensuring that a damaged or leaking sprinkler head does not harm equipment. When a fire alarm trips, the pipes fill with water. Then, heat sensors release water from only areas of the room that indicate heat caused by fire. This prevents the unnecessary release of water in areas where there is no fire threat. Also, when the fire is extinguished, the sprinkler head can automatically close to prevent excess water release. Consider including floor drains for quick removal of water. Make sure the drains include a backflow prevention system so that sewer water backups do not flood the server room.

Flood Considerations

In a flood, there is good news and bad news. The bad news is that there is not much you can do to prevent a flood. The good news is, at least you have less planning to do. Depending upon the cause, you might be able to prevent some types of flooding. For example, you could avoid placing the server room in locations where plumbing runs above or below the floor. A burst pipe could cause immense damage to server equipment. Also, remember to request floor drains with a backflow prevention system to prevent sewer backups into the server room while allowing fire sprinklers or other sources of water to evacuate.

If the flood is caused by a natural disaster, placing the server room as centrally as possible and away from exterior walls might allow other rooms to absorb the brunt of the initial water flow, although it may eventually reach the server room. General plumbing

principles dictate that your floor drains seldom work when a large-scale flood is in progress. Your flood disaster plan will primarily determine the best way to minimize damage and move equipment quickly, instead of trying to avoid the flood. In an evacuation plan, move anything storing data first—file servers and backup tapes in particular. A well-planned system design calls for redundant copies of data, so you probably have off-site copies of your data. However, off-site copies are usually not as recent as local copies. Even though the servers are expensive, they are replaceable—whereas the organization's data is probably not replaceable. Remember that much server equipment is extremely heavy and cannot be lifted by a single individual. Also, some server NOSs feature built-in redundancy. For example, the Windows 2000 Active Directory automatically replicates its database between domain controllers.

Be certain that your server equipment is adequately covered by an insurance policy.

Using Space Effectively

In addition to technical issues relating to servers and networking, other factors can affect your server planning. Some factors might be specific to your organization, and others might be common to most situations, as in the following list:

- *Choose a central location:* If you have a choice (as in new construction), try to locate the server room centrally (Figure 2-24). A central location makes it easier to provide good connectivity to the rest of the network and saves cabling costs. Try to design Internet and WAN traffic to and from your organization so that it flows freely and with as few intermediary devices as possible (switches or routers, for example).
- *Consolidate space:* The best way to get the most bang for the buck out of server floor space is to use racks and cabinets. (A cabinet is similar to a rack, except that it has a locked enclosure and cooling fans.) That way, you can store several pieces of equipment in a single horizontal floor space (Figure 2-25).
- *Restrict foot traffic:* Place the server room in a low-traffic area to minimize the risk of unauthorized access. Sometimes there are exceptions to this rule. For example, I recently visited a very large server manufacturer in Silicon Valley that displays parts of a server room through a window to a busy hallway. I didn't ask why they did this, but it seemed obvious that the company was proudly displaying its products to employees.

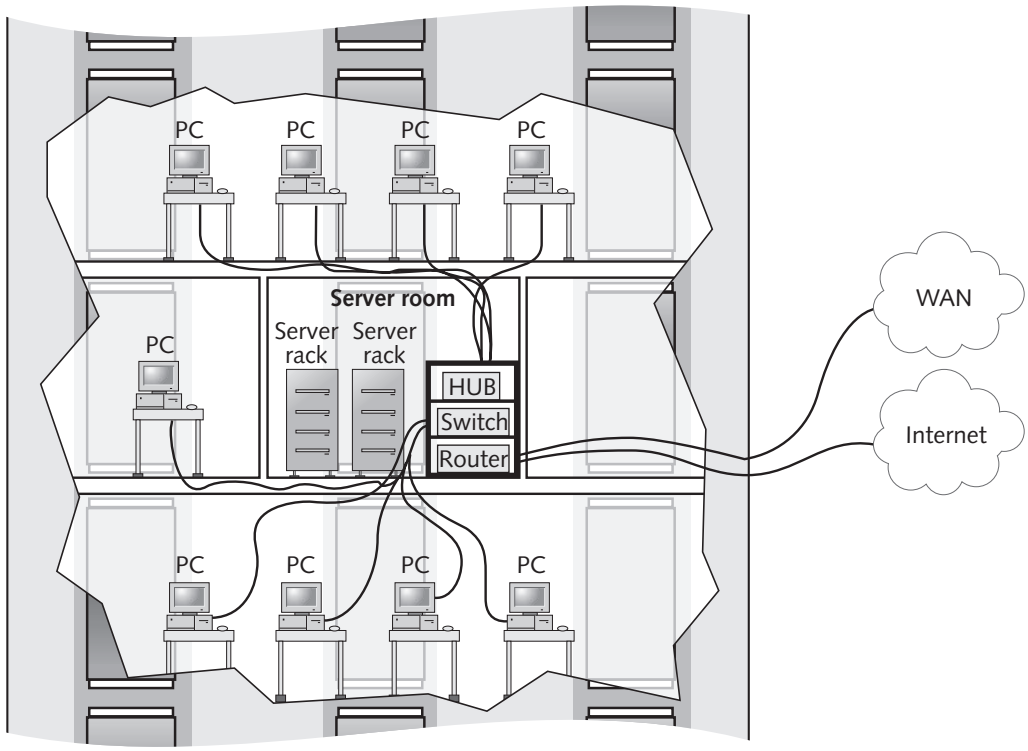

Figure 2-24 Centralize the server room for accessibility and reduced cable costs

- *Avoid exterior windows and walls:* Place the server room away from exterior building windows and walls for environmental and security purposes. In event of inclement weather, exterior windows might leak wind or rain, and sunlight contributes unwelcome warmth to the server room. A window that displays your server equipment to the outside world presents a security risk because someone can surmise much about your network design by viewing the equipment. Also consider that an evildoer could break the window and access the server room.
- *Be prepared to budget extra financing for server room design:* A server room is expensive. It requires expensive equipment and special design considerations. If you are responsible for budgeting the server room, bear this in mind and warn management in advance. As a general rule, you can multiply the cost per square foot of the building's general office space times four to arrive at the cost of server room space.

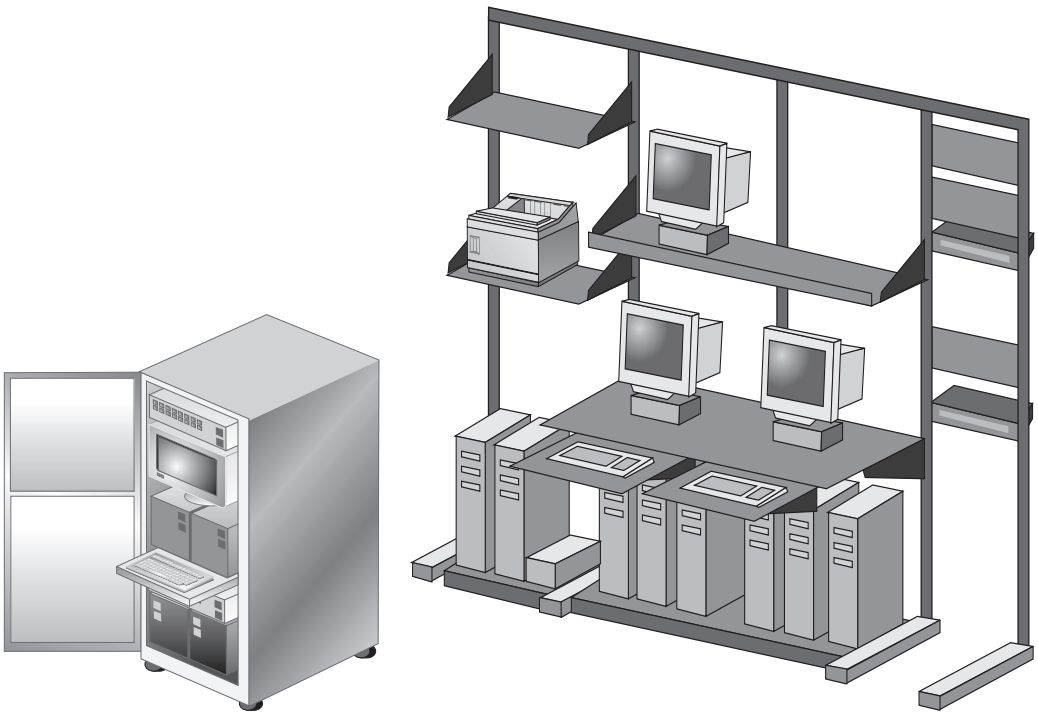

Figure 2-25 Cabinets and racks permit more equipment in the same space

Planning a Secure Location

Administrators of larger corporations are responsible for hundreds of millions and even billions of dollars worth of vital company data, such as customer databases, company secrets, accounting records, confidential employee records, and scores of other types of information—not to mention the value of the server equipment. Even if the organization is small, protecting company assets is still the administrator's vital concern. Securing the server room protects both the physical assets and the information stored on the servers. Although electronic security is designed to protect against hackers, viruses, malicious Internet users, and the like, physical security protects the actual server facility and equipment.

Physical security can be sophisticated, but it is not complicated. It is as simple as physical security has always been for everything from precious documents to currency—place the valuables in a safe and lock it. The server room is really a very large safe, and you as an administrator are responsible for ensuring that it is not accessed by unauthorized people. In fact, I know of a corporate contractor to the United States government that runs a server and a few highly secure workstations in a steel vault.

All other security measures are only as effective as the level of physical security. You might have extremely restrictive permissions and detailed auditing records on who can access company payroll records. While hackers are always a threat over the Internet or internal network, anyone with physical access to the server can utilize special utilities that allow access to the data stored on the hard disk even though they are not authorized for such access. For example, a utility known as NTFSDOS allows the user to boot the server from an MS-DOS floppy and gain complete control of the NT file system on an otherwise secure hard disk. Monitoring security starts with your own IT staff.

I Have Seen the Enemy …

And it is your own IT staff! A common source of company loss is employees, especially in the server room where there are a great many valuables. Instead of "borrowing a few paperclips," employees in the server room can "borrow a few memory DIMMs!" It is not up to me to tell you who to trust or to question your character judgment—just don't trust anybody. Sometimes, a security breach could be an innocent oversight—perhaps a new administrator provided a tour of the new server room to unauthorized outside persons. Or the security breach could be a deliberate, mean-spirited attack. Perhaps a disgruntled IT employee might want to seek revenge against the company before leaving for another job and, using his or her administrative privileges, destroys company data. It is wise to assume that anybody can steal or damage company assets—so implement sound security measures to remove or reduce such opportunities.

Always log off before leaving your computer. Otherwise, any passerby can access the local computer and network with the same authority you have, and any trace of improper activity will be logged to your account. Operating systems such as Windows NT or Windows 2000 allow you to lock your computer, requiring a password to unlock. Also consider logging on under only a general user account with no specific administrative privileges, and log on with administrative rights only when you need to perform administrative actions.

Restricting Access to the Server Room

As discussed earlier in this chapter, you should place the server room in an area that has minimal traffic. This minimizes the opportunity to access the server room and makes unwelcome visitors more obvious. Also, be very discriminating when determining who should see the server room. It is not a good practice to provide tours of the server room, even to employees of the organization. Next, make sure that the door you place on the server room is a solid, heavy, secure door made of solid wood, steel, or steel clad with a

heavy-duty lock. The type of lock you choose depends upon the level of security you want or can afford. A simple keyed lock might be sufficient; however, most organizations probably want more controlled access, such as the following:

- *Keypad:* Enter a number into an electronic keypad to unlock the door. This number might be a shared number that all IT staff knows, or it might be unique for each user. You should reset the number on a regular basis to ensure the secrecy of the number. A keypad provides minimal security because a passerby might be able to see a number as the user enters it.
- *Card scanners:* Issue authorized persons a card that is read by a scanner at the entrance to the server room. The cards are available in a number of formats. Some have embedded magnetic data that uniquely identifies the user. Others are smart cards that have digital certificates with metal contacts read by the scanner. These are nearly impossible to duplicate. Administrators can set conditions on the cards so that they grant access to the room only at certain times—to prevent employees from sneaking into the server room and performing malicious deeds when no one else is around, for example. When the scanner reads the card, an electronic lock unlocks the door for a few seconds. One of the only drawbacks to this system is that people tend to lose, misplace, borrow, or steal the access cards. Provide a written policy to your staff that specifies penalties for missing access cards. Also make sure that employees always wear the access card. Most cards include a photograph of the person, helping to ensure that only the person to whom the card was issued uses it.
- *Bio-recognition:* This is an emerging technology that verifies a person's identity based upon physical identifiers such as fingerprints, retinal scans, voice imprints, or some combination thereof.

For maximum security, require some combination of access methods. For example, employees might insert a smart card into a reader and also type a password. This method would ensure that the card was not stolen.

Monitoring Access to the Server Room

Despite your best security efforts, unauthorized persons might still find a way to access the server room, or authorized users might damage the server room. If such unfortunate occurrences take place, utilize a method of record keeping that allows you to know which persons were present at the time of the deed. Some of the following methods monitor access to your server room:

- *Sign-in:* Clearly the least secure method, a sign-in sheet depends upon the honor system, and persons that are a security risk are unlikely to be "honorable." A sign-in system should implement one or both of the next two methods that follow.
- *Security guard:* Because of the high cost associated with staffing a facility with a 24/7 security guard, this option might not be practical for all environments. However, a security guard adds an observer to unauthorized security

breaches and is useful for quick apprehension and prevention as well as adding a visible level of deterrence. A security guard might also check contents of all bags going into the server room.

- *Video surveillance:* Video surveillance captures activity in the server room or at the server room door 24/7. Some facilities keep video tapes indefinitely, but most rotate tapes on at least a seven-day schedule. Be sure to replace tapes periodically, because older, worn tapes do not provide a clear image. Video surveillance is only as good as the area it covers. If you cover the server room, be sure to also cover wiring closets, areas where you store backup tapes, and so forth.
- *Logs:* Most controlled access methods such as scanners or electronic keypads keep logs that show who entered the server room and when. In addition, you can configure the NOS to track certain resources so that if someone attempts to access a resource (whether successfully or unsuccessfully), a log records the name of the logged-on user and time and date of access.

In securing the server room, do not forget to also secure other sensitive, physically accessible areas. You should, for example, secure patch panels and wiring closets, which provide a point of convergence for network cabling, making it easier to manage. In seconds, someone could access an exposed patch panel and start ripping out cable, causing considerable damage to network operations. Also, place backup media in secured data storage areas to prevent stolen tapes. In the IT context, your organization is not the server room; it is the data. Stolen tapes are a severe security risk. Secure the telco room, which is the access point for telephone communications and often shares its connections with a WAN or Internet connection.

Further secure the contents of the server room by placing locks on server equipment. For example, most server cabinets require a lock, and you can optionally lock individual components of the server rack. One reason for rack-mounted equipment is easy portability from one rack to another. However, you do not want someone easily porting the equipment into a backpack or briefcase. Do not leave spare parts lying around—secure them in a locked cabinet as well, and record parts with serial numbers.

Chapter Summary

- Increasingly, organizations are looking for network administrators who not only have computer and network expertise, but also know how to get the most value for every dollar spent in servicing the network.
- Ask the following questions about server needs: Do we really need this server right now? Is the expense of the server offset in savings? Is the timing of a server purchase appropriate? Is there sufficient expertise available to run and service the server?

- Ask the following questions about fulfilling user requirements: How many users will connect to the server? What is the nature of user access? Should users be able to access the server directly? As a rule, assume that users do not require direct server access and take measures to prevent such access unless you know users or groups of users that require a specific level of access. Also, user access to the server should only be from workstations across the network; users should never log on locally to a server.
- In planning for interoperability, the administrator must ensure that operating system platforms can interoperate with one another and that the user experience is not disrupted.
- Installing a server involves much more than finding an empty space, plugging it in, and installing the operating system. You must also place the server so that it serves users in the network design in the best possible way. In a global enterprise, also consider factors such as the site links and bandwidth utilization within and between networks.
- A network diagram is a physical and/or logical representation of the network, also known as a network map. You create a network diagram to design a network, keep a record of the network, or assist in changing or troubleshooting a network.
- Physical site readiness is one of the most critical aspects in determining where to place servers, and involves controlling temperature, humidity, and dust.
- Keeping server equipment cool requires adequate airflow and redundant air conditioners that are independent of general-use air conditioners.
- Good server room air quality requires efficient filtration both in the HVAC system as well as in the ventilation of the internal server components. Filtration prevents a buildup of dust, which contributes to overheating.
- High humidity can lead to condensation with sudden temperature changes and accelerates buildup of corrosion on metal components. Low humidity increases the risk of ESD.
- Use static-resistant, commercial-grade floor tiles in the server room. Avoid carpet, which increases the risk of ESD. A flat floor requires a ceiling plenum to run cable, power, and HVAC.
- A raised floor design allows for a floor plenum and provides excellent grounding to avoid ESD. HVAC vents in the floor provide excellent cooling when directed up through server racks.
- There are three sources of power to the server room: the main power, the uninterruptible power supply (UPS) for temporary situations, and the backup generator power for extended, system-wide outages. Clean power extends the life of the server and its components. "Clean power" means the absence of surges, spikes, dips, or poor grounding, which can lead to short circuits, tripped electrical breakers, and possibly damage to equipment or people. Electromagnetic interference (EMI) is a byproduct of electricity, can disrupt or corrupt data traveling along network cable, and can disrupt other electrical equipment.

- While smoke detectors provide a warning for fire, chemical extinguishers suppress the fire without damaging equipment. When using chemical extinguishers, be sure to also provide quick ventilation to expel the chemicals after the fire. Alternatively, a "dry" extinguishing system uses water but only fills the pipes when there is a fire.
- Strategically place plumbing away from the server room ceiling and floor, and make sure floor drains include backflow preventers.
- In an evacuation plan, move anything storing data first—file servers and backup tapes in particular. Even though the servers are expensive, they are replaceable, whereas the organization's data is probably not replaceable.
- In using space effectively, consider the following factors: Choose a central location, consolidate space, restrict foot traffic, avoid windows and walls, and prepare to budget extra financing for server room design.
- It's important to physically secure the server room and important networking equipment. A common source of company loss is the employees, especially in the server room, where there is a lot of valuable data and equipment. In addition to a solid locked door, consider controlled access methods such as keypads, card scanners, and bio-recognition devices. Also, monitor access to the server room using a sign-in sheet, security guard, video surveillance, and logs. Further secure the contents of the server room by locking server racks and cabinets.

Key Terms

bandwidth — The transmission capacity of the network. For example, most Ethernet networks can transmit 10 Mbps or 100 Mbps.

datacenter — A term with two meanings, depending upon the context. It can refer to a consolidation of the majority of computer systems and data into a main location, or it can refer to one or more very powerful servers optimized as database servers—sometimes configured with as many as 32 processors.

electrostatic discharge (ESD) — Static electricity that can damage, destroy, or shorten the life of the server's electrical components.

enterprise — A geographically dispersed network under the jurisdiction of one organization. It often includes several different types of networks and computer systems from different vendors.

failover — If one server fails, the remaining server(s) continue to provide service.

File Transfer Protocol (FTP) — A TCP/IP protocol that manages file transfers. Usually used to download files over the Internet.

inter-site communication — Communication between hosts in different sites, such as over a WAN link.

intra-site communication — Communication between hosts within a single site, often over a LAN.

Linux — A version of UNIX that operates on PCs as well as Alpha RISC and PowerPC platforms.

load balancing — Distributing a network role between two or more servers.

network interface card (NIC) — The workstation's adapter card that connects to the network and through which network communication takes place.

network utilization — The percentage of bandwidth in use in a given period of time.

noncondensing relative humidity — Absence of moisture accumulation, such as on the outside of a cold glass.

Novell Directory Services (NDS) — A hierarchical database of network resources that allows users from anywhere in the enterprise to access resources throughout the organization, as opposed to logging on to a single server and accessing only resources available from that server.

oversubscribe — A network connection with network utilization that exceeds an acceptable baseline for the available network bandwidth. The network utilization has a direct relationship to network bandwidth: the higher the network bandwidth, the lower the network utilization.

plenum — The space between the dropped ceiling tiles and the actual ceiling, or the space between the raised floor surface and the concrete.

positive pressure — The internal environment of a server case or cabinet that utilizes one or more filtered fans to supply main internal airflow throughout the server. Internal server fans only draw upon this filtered air.

router — A device that divides the network into separate parts and forwards network traffic to appropriate destinations.

single sign-on — A single logon that allows transparent access to multiple servers. For example, a single sign-on might allow you to log on to a NetWare server and pass the logon credentials to an NT 4.0 server as well.

site — The LAN(s) on either side of a WAN connection.

subfloor — A space between the concrete floor and the floor tiles; also known as the plenum.

subnet — A division in the network useful for limiting network traffic to a particular location; also known as a segment in many contexts.

synchronize — The process of making data in one location consistent with data in another location. Synchronization is necessary to ensure that user accounts, for example, are consistent from one logon server to another. Synchronization also applies to items such as data files.

transistor — An electronic device that opens or closes, or turns on or off to provide a logic gate or switch. Transistors provide the "thinking" capability of the processor.

uninterruptible power supply (UPS) — A device that supplies power temporarily to allow administrators to perform a graceful shutdown of server equipment. Otherwise, the sudden loss of power to the server can be extremely damaging to the operating system, applications, and open data files.

UNIX — An open server operating system that allows vendors to specially modify it to their servers. UNIX usually operates on more expensive RISC-based processors.

WAN link — The telecommunications connection that links the various networks that comprise parts of a wide area network (WAN).

web farm — Multiple web servers providing the same web content.

Review Questions

1. You have a very limited budget, but the email server failed. What should you do?
   a. Replace the failed server or the failed component(s).
   b. Convert the corporation to Internet mail only.
   c. Use paper memoranda until you have more money.
   d. Use a user's workstation as an email server.
2. What does load balancing do?
   a. distributes a network role between two or more servers
   b. evenly distributes server weight on a raised floor
   c. evenly distributes power load between breakers
   d. evenly distributes WAN traffic between multiple links
3. Bandwidth is:
   a. a measure of electromagnetic interference
   b. the percentage of network utilization in a given period of time
   c. the average amount of data that can be transmitted in a given period of time
   d. the transmission capacity of the network
4. Network utilization is:
   a. the transmission capacity of the network
   b. the number of hosts on the network as a percentage of the maximum allowed number of hosts on the network
   c. the percentage of bandwidth in use in a given period of time
   d. the amount of bandwidth required to upload or download a large file
5. Which of the following would be a reasonable justification to add a more expensive, higher-bandwidth WAN link?
   a. The existing WAN link is oversubscribed.
   b. The existing WAN link is undersubscribed.
   c. The existing WAN link is used only for nightly synchronization.
   d. to increase the number of users that can log on across the WAN link

6. The administrator provides what to the users?
   a. a service
   b. endless ridicule
   c. only what the user asks for
   d. troubleshooting expertise when users damage their computers
7. Which of the following could be good reasons for using differing operating systems? (Choose two.)
   a. merging of two companies with different operating systems
   b. Some users like one type of NOS while others like another.
   c. It is better to have separate user logons to each operating system to improve security.
   d. You require the features of a particular operating system and you also have an application that only works on another operating system.
8. Linux is a version of:
   a. NetWare
   b. OS/2
   c. Windows
   d. UNIX
9. You should put the server room:
   a. on the bottom floor of a multiple-story building
   b. on the top floor of a multiple-story building
   c. furthest away from the incoming WAN and Internet links
   d. as centrally as possible
10. Why would you want to create a network diagram? (Choose all that apply.)
    a. to express yourself artistically
    b. to assist in locating equipment when you need to troubleshoot
    c. to use as a tool to justify your budgetary expenditures
    d. so users know which servers are closest to them
11. Why is a server room hotter than other rooms in the building?
    a. Electrical components generate heat.
    b. It is hotter by design to reduce humidity.
    c. Optimum placement by exterior windows allows heat from sunlight.
    d. It is designed to make people uncomfortable.

12. Besides fans in server equipment and cabinets, what can you do to keep the server room cool?
    a. Prop the server room door open at all times.
    b. Add one or more dedicated air conditioners to the server room.
    c. Add oscillating fans wherever possible.
    d. Open a window.
13. Why is a lack of adequate humidity detrimental to the server room?
    a. It increases EMI.
    b. It might cause electronic circuitry to crack.
    c. It causes expansion and contraction of server components.
    d. It increases chances of ESD.
14. Why is dust in the server room a problem?
    a. Dust accumulation creates an unprofessional appearance.
    b. Dust acts as an insulator, increasing heat problems.
    c. Dust particles can adversely affect moving parts.
    d. Dust is no more a problem in the server room than it is in other rooms.
15. A positive pressure environment:
    a. provides filtered air to internal server cooling fans
    b. encourages people to do good deeds
    c. forces filtered air into the server room at a greater rate than it escapes
    d. is a server room condition that occurs when temperature, humidity, and dust control are all within acceptable parameters
16. High humidity can cause:
    a. mold spores on server components
    b. increased occurrences of ESD
    c. increased occurrences of EMI
    d. corrosion on metal components
17. A raised floor is advantageous for which of the following reasons? (Choose all that apply.)
    a. makes the ceiling closer, thereby easier to service the ceiling plenum
    b. excellent grounding to avoid ESD
    c. provides plenum space for cables, power, and HVAC
    d. handy plenum space for storing spare parts

18. Why should you use a UPS even if you already have a reliable backup generator?
    a. The backup generator can only run for a few minutes.
    b. The backup generator might not provide clean power, and the UPS can condition the power as necessary.
    c. Backup generators normally serve the general building, not the server room.
    d. The backup generator requires about 15 minutes to start—the UPS provides power in the mean time.
19. Why might you choose to install a dry system for fire suppression?
    a. to avoid water in event of a broken or leaking sprinkler head
    b. to avoid rust
    c. to reduce the weight of pipes in the plenum
    d. to avoid use of harmful chemical-based fire-suppression systems
20. In case of a flood, what should you first attempt to move to a safe location?
    a. the mainframe
    b. spare parts
    c. anything storing company data
    d. the Chia Pet

HANDS-ON PROJECTS

Web links in projects were accurate at the time this book was published. If you notice discrepancies, look for similar links and follow the same general steps.

Project 2-1

Three departments have specific network problems, as shown in Table 2-1. You intend to solve the problems with the equipment shown. However, your budget is extremely slim and you will have to request additional funding to purchase equipment. Your supervisor asks you to prioritize each item. In the Proposed Equipment column, write the number 1, 2, or 3 to represent the highest priority (1), second highest (2), and the lowest (3).

Table 2-1 Priorities of Proposed Equipment

Department	Problem	Proposed Equipment
Data Processing	Slow response in processing user queries; however, functionality is 100%.	New server with four processors
Administration	Email server is heavily utilized and frequently stops responding. Day-to-day operations heavily dependent on email.	Two new clustering email servers
Research & Development	Approaching full disk space. You predict it might take a few more weeks before a critical shortage occurs.	New file server

Project 2-2

Using your web browser, access *www.novell.com*. This is an exceptionally well-designed site in most respects, and in your career as a network administrator, you should be able to use it to find information fairly quickly. Locate and read about the Client 4.8 for Windows NT/2000 download.

1. Describe how this download helps Microsoft Windows NT/2000 and Novell NetWare to interoperate.
2. Look for a note to Innoculan users—what does it say? (Innoculan is a virus-detection utility.) What should you do to remedy the problem with Innoculan?

Project 2-3

NTT India is an Internet and intranet solutions company. NTT hosts web sites for their clients on their servers. Of course, the servers must have significant uptime and failover protection. Access *www.nttindia.com,* click the Servers link, and answer the following questions:

1. What operating system does NTT use?
2. What components on their servers are hot-swappable?
3. Describe the force-filtered cooling of NTT servers.
4. What type of redundant power system does NTT use?
5. What temperature does NTT maintain in their server room?
6. How does NTT control access to the server room?

Project 2-4

Data Clean Corporation provides cleaning services for controlled environments such as server rooms. Using your web browser, access *www.dataclean.com*. Click the services link, read the web page, and then answer the following questions:

1. Why is it important to have the floor plenum cleaned?
2. What is important about cleaning the floor surfaces?

Project 2-5

The Liebert Corporation provides a variety of environmental control solutions. Using the Liebert web page, find information about air conditioning and airflow.

1. Using your web browser, access *www.liebert.com*.
2. Click the **Computer Rooms** link.
3. Click the **Precision Cooling** link. The Computer Rooms page displays a Precision Cooling column.
4. Click the **precision air conditioning** link.
5. Scroll down to the High Capacity section, and click the **Deluxe System 3–60Hz** link.
6. Under Support Documents, click **Brochure (4pg) - Upflow Applications (R 11/98) - 23KB** and read the document (click **Next** at the bottom to access all the pages).
7. On the second page, which of the airflow methods is specifically designed for a raised floor?
8. Exit the web site and your browser.

Project 2-6

Because halon is being phased out, consider other alternatives for chemical fire-extinguishing needs, such as those manufactured by DuPont.

1. Access *www.dupont.com/fire*.
2. Play the AVI video clip link **Burning Heptanet 10B Pan Extinguished by FE-36**. Although FE-36 is used in portable hand-held fire extinguishers, its effectiveness in extinguishing a fire is similar to the effect of other chemical extinguishers. (Note: this video clip is 1.5 MB, so if your Internet connection is slow, you might have to be patient.)
3. From the *www.dupont.com/fire* page, click the **Alternatives** link (*www.dupont.com/fire/products/index.html*).
4. Click the link for FE-13. What are a few reasons that FE-13 would be good for use in server rooms?

CASE PROJECTS

1. You have started a new job as the manager of network administration for a medium-sized company in Phoenix. This company has had several managers in your position through the years, and each one has favored one operating system over another. As a result, you have several Intel CISC-based computers running several versions of Linux, NetWare 4.2, NetWare 5.1, Windows NT 4.0, and one server running IBM OS/2. Desktop workstations run Windows 95, Windows 98, Windows NT 4.0 Workstation, and IBM OS/2. The company's other office is located in San Francisco and is only a satellite office with no servers. The users in the San Francisco office complain that they must use a dial-up connection to access the Linux server at your office. Your first assigned task is to standardize the entire environment as much as possible. In your opinion, Windows 2000 is easiest from the end-user perspective and also provides effective management tools. What can you do to standardize the operating systems while resolving the San Francisco users' complaint about using a dial-up connection to your office?
2. In your first week on the job described in Case Project #1, you find that there isn't a server room. Instead, as the company grew, each department added their own servers in utility or storage closets. You know that because a server room was not designed into the original building plans, you might not be able to install the server room of your dreams. However, there is a centrally located break room that is not used much because the company has a new cafeteria. You have permission to use this room and have hired a construction company to provide architects and engineers who will help you migrate all servers to the central location. What kinds of requests in terms of physical site conditions, power supplies, disaster planning, and security will you make to the architects and engineers?